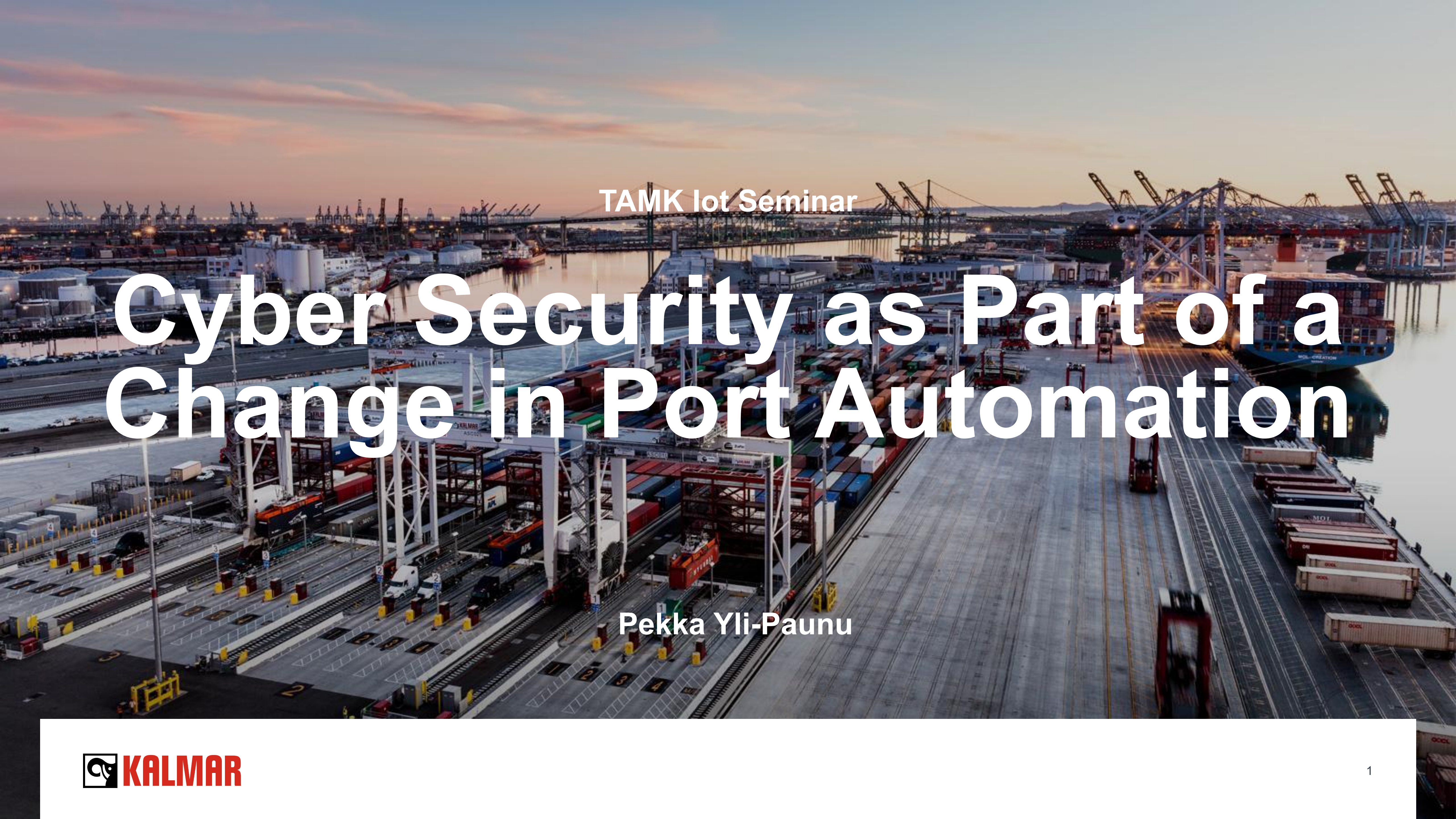


TAMK Iot Seminar

Cyber Security as Part of a Change in Port Automation

Pekka Yli-Paunu

Introduction

The wave of data collection, sharing and utilization to optimize operations via automation is the next phase of industry revolution, **Industry 4.0**. The convergence of real and virtual worlds as a result of digitalization has been a crucial driver of change and innovation in the sea port sector.

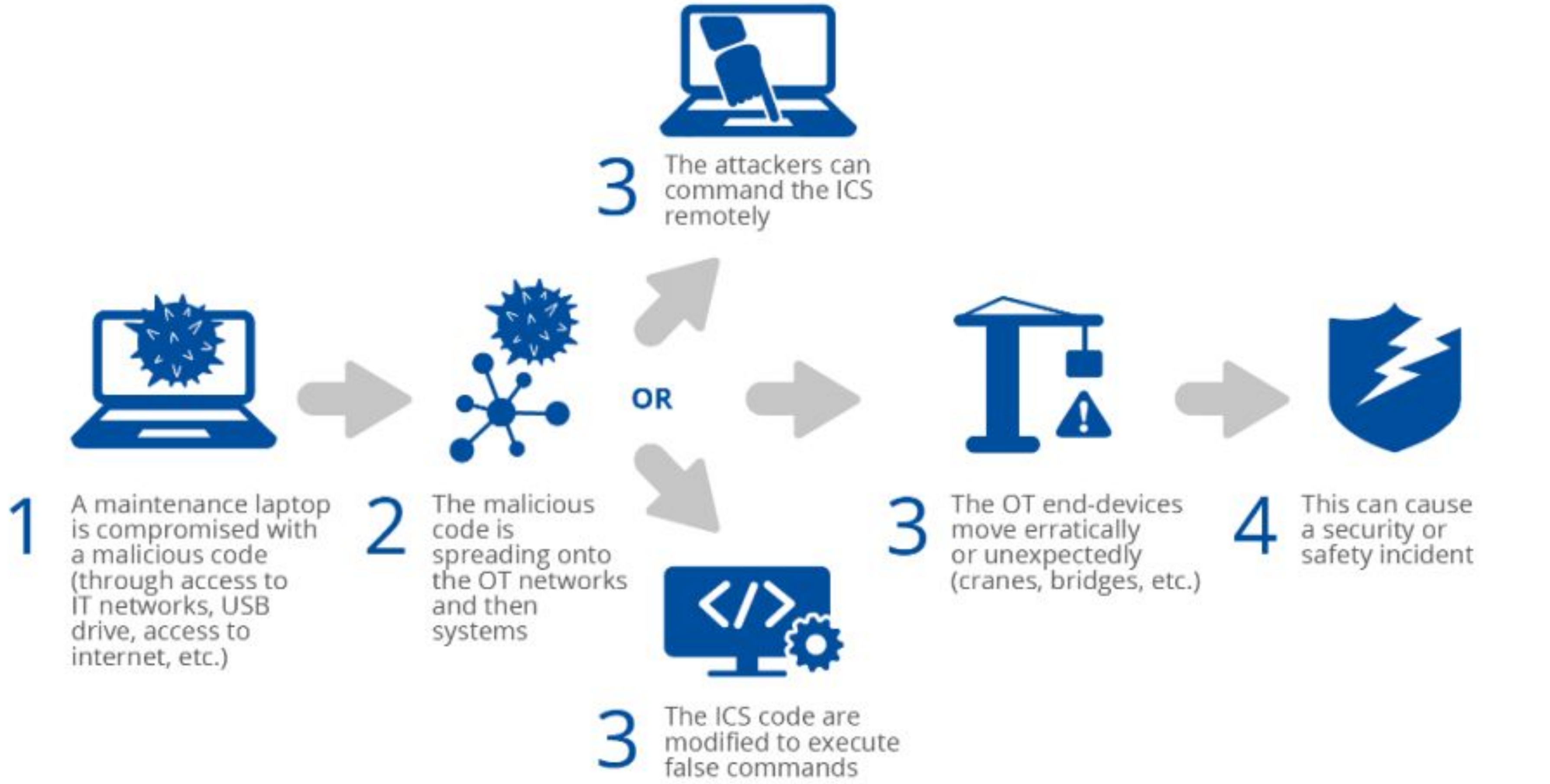
Data has been elemental in developing sustainable mobility and logistics helping big companies, securing a competitive position. The Age of Industry 4.0, which is based on **platform based cooperation** between liners, ports and logistic service providers and innovation based strategy incorporating weather and traffic data to optimize operation exposes companies to many challenges.

Cyber Security Challenge

Apart of the traditional nature of port industry which is inert to changes, **the introduction of disruptive technology** amalgamated with the competitive nature to be the first mover in a data driven and interconnected ecosystem, exposes all the players to a multi-dimensional cybersecurity threat.

Logistical (machine automation, Container tracking) and infrastructural (Port operations, fleet management) systems are under a tremendous risk of cyber attack.

Cyber Security Challenge



1 A maintenance laptop is compromised with a malicious code (through access to IT networks, USB drive, access to internet, etc.)

2 The malicious code is spreading onto the OT networks and then systems

OR

3 The attackers can command the ICS remotely

3 The ICS code are modified to execute false commands

3 The OT end-devices move erratically or unexpectedly (cranes, bridges, etc.)

4 This can cause a security or safety incident

KALMAR

Cyber Security is a Risk in Port Industry

A clustered industry consisting of manufacturers, owners, operators, port authorities, logistic service providers, the container sector which generates enormous amount of data, is vulnerable to cyber risk which not only threatens security but also the safety of the container handling machines.

Information technology (IT) and operational technology (OT) in the sector are increasingly being networked together. This not only pose data security threats but also **safety risks**. The Petya-Ransomware for example, an untargeted attack disrupted all of Maersks operations in 76 ports on 27th of June, 2017.

The affects on Maersk Line, one of the front-runners in IT-development, is a warning sign to the entire port industry.

Cyber Security is a Risk in Port Industry

In an asset heavy and capital intensive industry with innumerous moving parts, the system with a large number of end users is wide-open to untargeted (Phishing, water holing, ransomware) and targeted (Spear-phishing, Deploying Botnets, Subverting system) attack

The risk of **autonomous vehicles** with systems including software to run engines, control and information system, global position system et al are highly vulnerable to hostile takeover or disruption of operating ability.

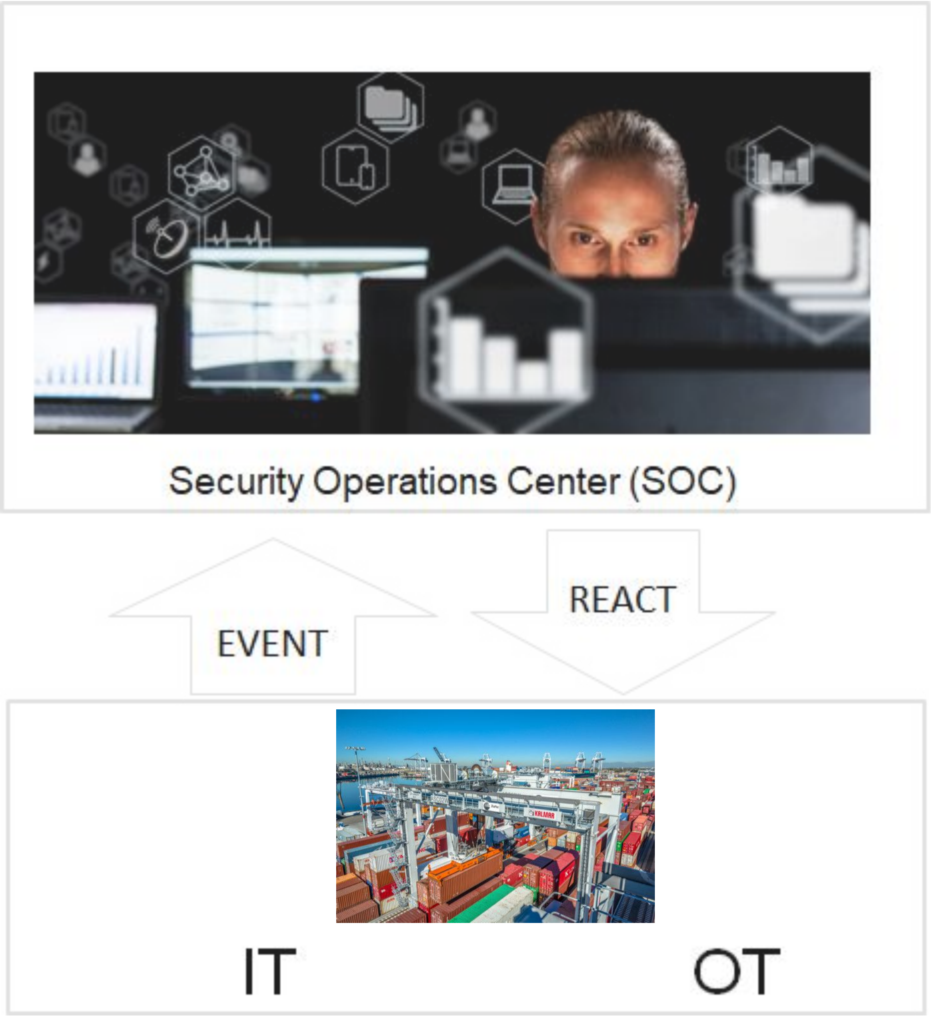
Hacktivist can hack systems, and minor changes like path planning can risk the physical safety of the machines.

Addressing cyber infrastructure and investing to safeguard port industry is crucial in the changing ecosystem.

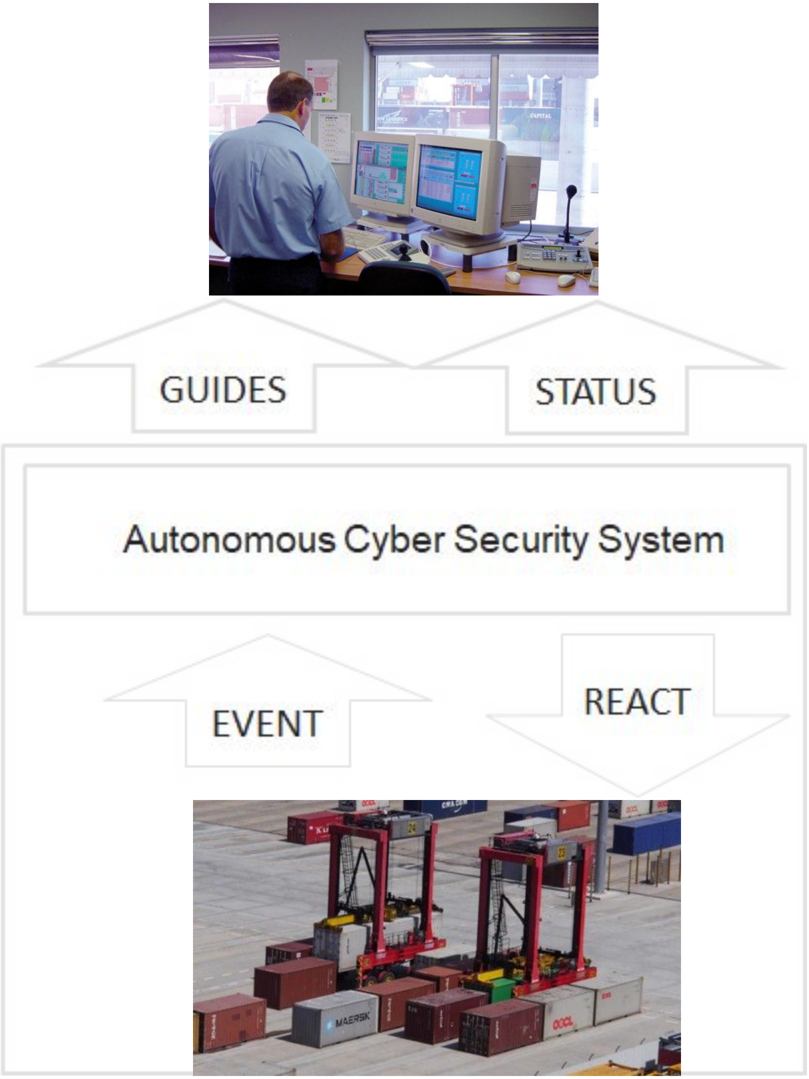
Kalmar Studies

Autonomous Cyber Security System

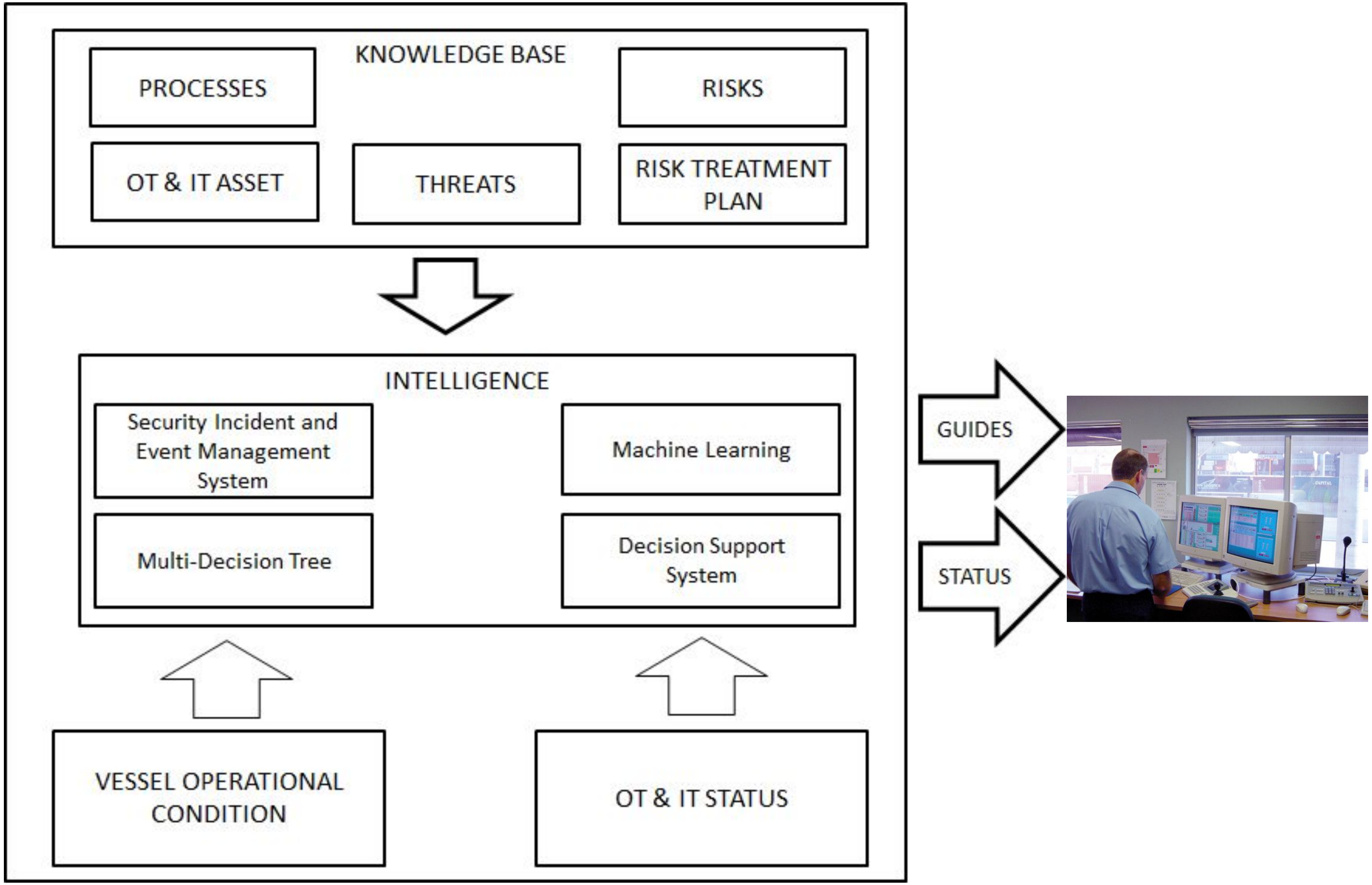
Common model



Autonomous model



High Level Architecture



KNOWLEDGE BASE

PROCESSES

RISKS

OT & IT ASSET

THREATS

RISK TREATMENT PLAN

INTELLIGENCE

Security Incident and Event Management System

Machine Learning

Multi-Decision Tree

Decision Support System

VESSEL OPERATIONAL CONDITION

OT & IT STATUS

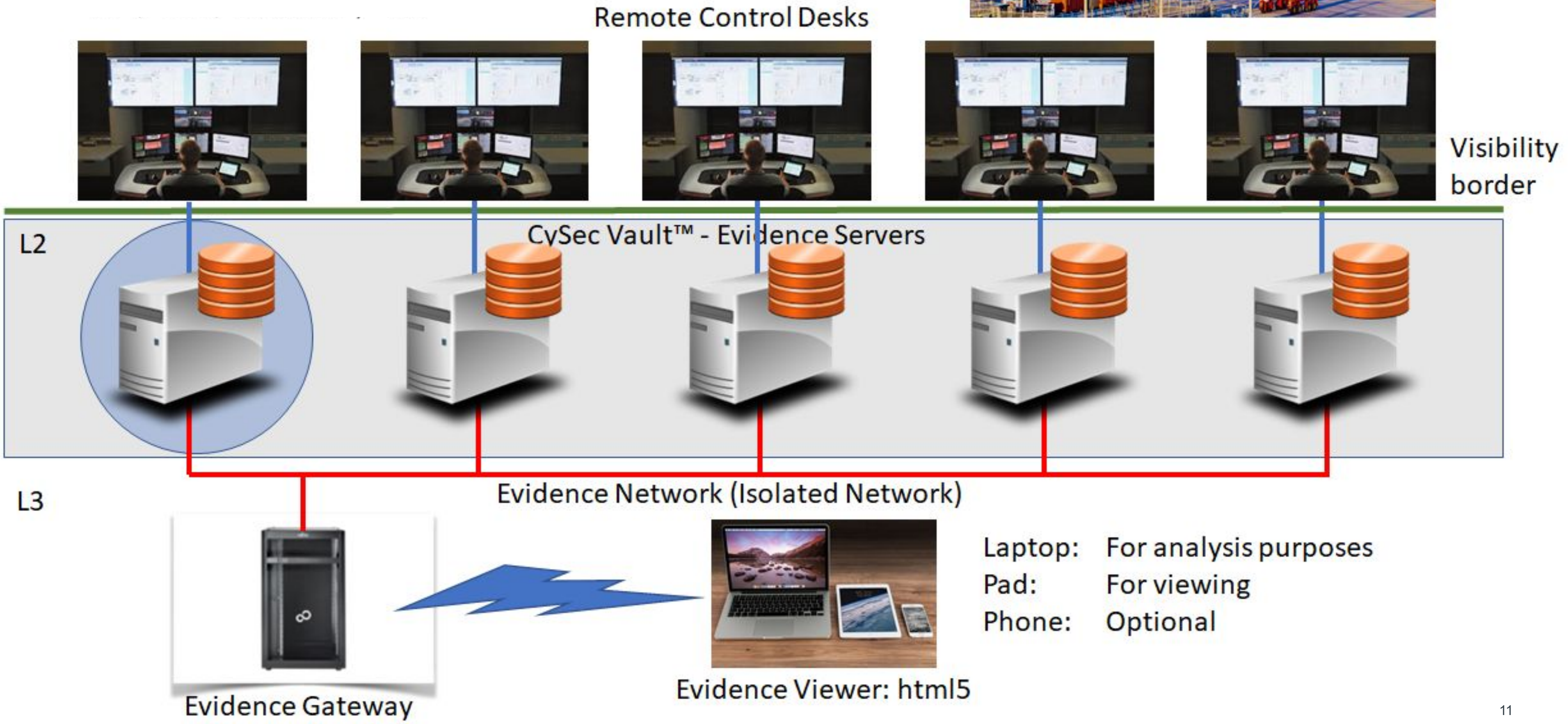
GUIDES

STATUS

CySec Vault

CySec Vault™ (CV), a part of the CySec Ice Wall platform, is a patented autonomous Network-Evidence-Acquisition System that continuously collects and preserves vast amount of customer’s live high-risk Internet or intranet traffic into multipurpose or virtual servers, and clouds. CV is an essential part of an **evidence discovery platform**.

Evidence Architecture



Remote Control Desks

Visibility border

L2

CySec Vault™ - Evidence Servers

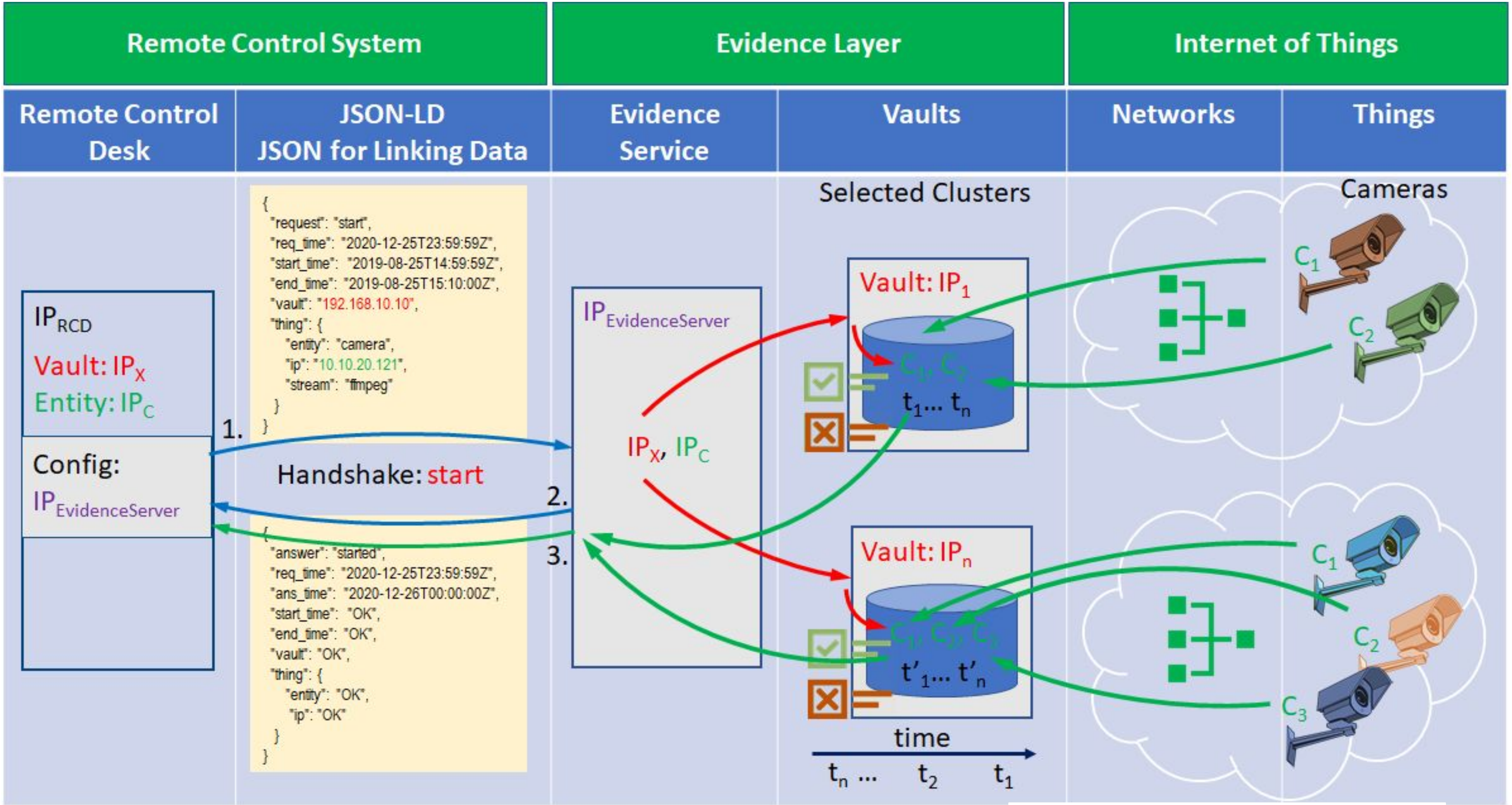
L3

Evidence Network (Isolated Network)

Evidence Gateway

Evidence Viewer: html5

Laptop:	For analysis purposes
Pad:	For viewing
Phone:	Optional



Remote Control System		Evidence Layer		Internet of Things	
Remote Control Desk	JSON-LD JSON for Linking Data	Evidence Service	Vaults	Networks	Things

```
{
  "request": "start",
  "req_time":  "2020-12-25T23:59:59Z",
  "start_time":  "2019-08-25T14:59:59Z",
  "end_time":  "2019-08-25T15:10:00Z",
  "vault": "192.168.10.10",
  "thing": {
     "entity":  "camera",
     "ip": "10.10.20.121",
     "stream":  "ffmpeg"
  }
}
```

Handshake: start

```
{
  "answer": "started",
  "req_time":  "2020-12-25T23:59:59Z",
  "ans_time":  "2020-12-26T00:00:00Z",
  "start_time":  "OK",
  "end_time":  "OK",
  "vault": "OK",
  "thing": {
     "entity":  "OK",
      "ip": "OK"
  }
}
```

KALMAR

Mitigating Cyber Risks

As an industry moving towards a connected **cloud based environment** cyber security becomes fundamental element of risk management.

In a hyper-dependent supply chain, cyber risk are systemic and disruptive due the domino effect. There is an urgent need to dwell in **regulating and standardizing** cyber safety.

Most organization can tackle cyber security threats using the current tools, but it’s often a matter of ensuring systems are **update and security features are regularly tested** (Informa Group, 2017). This requires resource availability and allocation, which in turn highlights the need for **training** personal and expanding IT teams

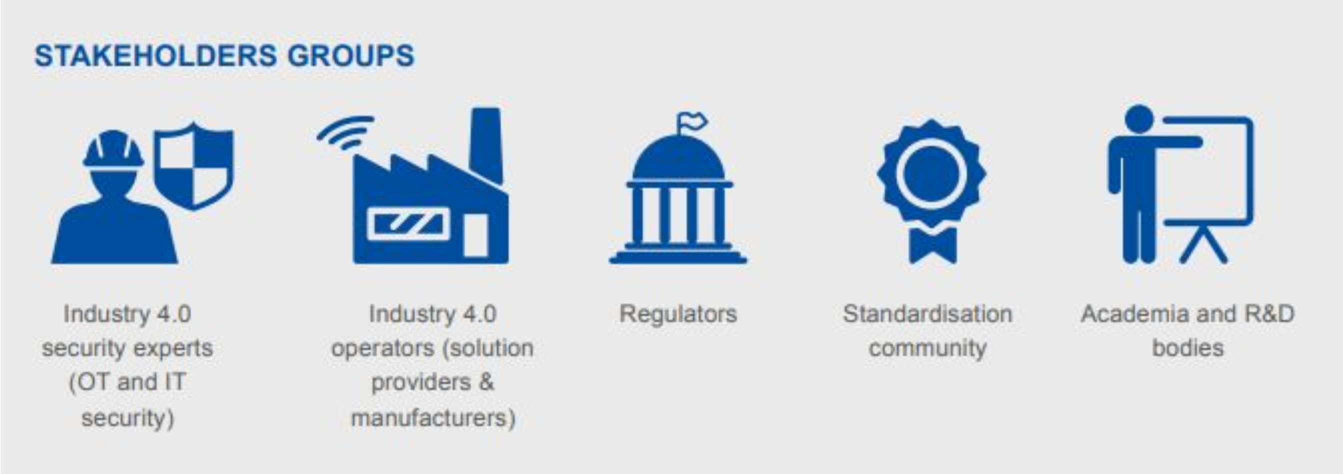
Cargo management system and power control systems in ports are at risk and terminal operators should upgrade systems not only to improve efficiency but also safety.

Mitigating Cyber Risks

Regulatory steps to standardize equipment (port machinery) and backups systems to mitigate hacking or disruptive threat would be essential to ensure safety and security.

Policies and procedures to conduct risk analysis and upgradation of IT systems at regular intervals, safe disposal of hard drive, authorization requirement for remote access and an incremental protective framework based on operational significance, should be developed.

An increased use of **open-data, and Internet of things** will increase the data available to hackers, a risk versus reward approach would point towards a top-down cyber safety approach.


STAKEHOLDERS GROUPS
Industry 4.0 security experts (OT and IT security)
Industry 4.0 operators (solution providers & manufacturers)
Regulators
Standardisation community
Academia and R&D bodies

Conclusions

A safety and security matrix in the port industry which is constantly moving towards digitalization comprises more than just physical threats to safety and security.

Cyber security risk management is becoming **a crucial component** of the port sector and the global supply chain.

Still at a primitive stage, IT systems have a lot of **room for improvement**.

Stakeholders need to take steps to ensure their systems are secure, vigilant and resilient as discovering the threat and recovering from it quickly is paramount to reduce losses.

There is a need to devise regulations and protocols as soon as possible, as the pace of digitalization in the industry and the **ever-changing threat landscape** has the potential to create massive disruption as ports are a part of critical infrastructure.

Conclusions

Companies and authorities should upgrade system to secure infrastructure, protect data, customers and employees.

End-user are most prone to such attacks and steps need to be taken to improve IT and OT system protocols.

Developing in-house IT system might not be economically possible for all parties and third party IT risk assessment companies and tools are useful.

As the port industry sector casts itself into the Industry 4.0 setting, port organizations are underprepared to handle attacks from hackers and **it is high time to moved away from legacy systems to dynamic cyber specific systems**.

Making your every move count.